WE CLAIM:

1. A system for authenticating a customer transaction on a electronic network, the system comprising:

an access device for customer access to the electronic network;

an integrated circuit chip that is issued to the customer and contains customer-identifying data;

a reader that is linkable to the access device and can communicate with the chip;

and

an authentication request server (ARS) that in conjunction with an Access Control Server (ACS) is linked to the electronic network and can communicate with a party requesting authentication of the transaction,

wherein the ACS is configured to communicate directly with the customer's access device for authentication of the transaction bypassing a need for authentication software downloads from the requesting party to the customer's access device,

wherein the ARS is configured to receive transaction information from the requesting party and to communicate transaction data to the reader via the customer's access device,

wherein the reader is configured to receive the transaction data and to communicate a value based on the transaction data to the chip,

wherein the chip is configured to generate a cryptogram based on at least a portion of the transaction data and at least a portion of the customer-identifying data on the chip,

wherein the reader is further configured to communicate an authentication token based on the cryptogram to the ARS, and wherein the ARS is further configured to evaluate customer-identifying data from the authentication token and to validate the authentication token for authentication of the customer transaction.

2. The system of claim 1 wherein the transaction data communicated to the reader comprises a challenge based on the transaction information.

3. The system of claim 1 wherein the authentication token has a format that is compatible with 3-D Secure protocol message formats.

4. The system of claim 1 wherein the authentication token upon successful evaluation by the ARS results in generation by the ACS of an Accountholder Authentication Value (AAV) that is transported on the electronic network in an Universal Cardholder Authentication Field (UCAF) which has a 20 byte length.

5. The system of claim 1 wherein the chip and the reader are co-disposed in a single physical package.

6. The system of claim 1 wherein the access device, the chip and the reader are co-disposed in a single physical package.

7. The system of claim 1 wherein the ARS is configured to evaluate customer-identifying data from the authentication token by first rebuilding the data used by the chip to generate the cryptogram, next generating a replica cryptogram from rebuilt data, and then matching the authentication token with the replica cryptogram.

8. The system of claim 1, further comprising a cardholder database that can be accessed by ARS to retrieve stored customer information.

9. The system of claim 1 in which the ARS is further configured to communicate an authentication result to the requesting entity.

10. The system of claim 1 wherein the ARS is further configured to match an application transaction counter received from the chip against previous values of the application transaction counter received from the chip and to accordingly authenticate the transaction.

11. A system for authenticating a customer transaction in a 3-D Secure compliant electronic network environment, the system comprising:

a merchant;

an issuer;

an acquirer for accepting transaction specific data from the merchant and transferring data to the issuer;

an Authentication Request Server (ARS) operated by the issuer in conjunction with an Access Control Server (ACS);

a Cardholder Authentication Page providing an interface between the ACS and the customer;

an EMV – compliant chip card issued to the customer by issuer, the chip card having customer identification data; and

a reader for communicating with the chip, wherein the reader is linkable to the Cardholder Authentication Page,

wherein the chip card and the reader are configured to generate an authentication token based on a cryptogram of at least a portion of the customer identification data and at least a portion of transaction specific data received by the reader via the Cardholder Authentication Page,

wherein the ARS is configured to evaluate the authentication token for validation, and wherein the validation of an authentication token results in the generation of an AVV which is transported on the electronic network in an UCAF that has a 20-byte length.

12. The system of claim 11 wherein the chip and the reader are co-disposed in a single physical package.

13. The system of claim 11 wherein the Cardholder Authentication Page, the chip, and the reader are co-disposed in a single physical package.

14. The system of claim 11 wherein the chip card generates the cryptogram in response to EMV standard commands issued by the reader.

15. The system of claim 11 wherein the chip card comprises a bitmap mask selected by the issuer to identify specific bits of the cryptogram that are included by the reader in the authentication token.

16. The system of claim 11 wherein the ICC is programmed to generate the authentication token in conjunction with the reader after verification of a personal identification code entry by the customer.

17. The system of claim 11 wherein the ICC is programmed to generate the authentication token in conjunction with the reader after the customer verifies a transaction amount.

18. The system of claim 11 wherein the ACS is configured to display the Card Authorization Page as a pop-up or in-line web page for communicating data and instructions to the cardholder.

19. The system of claim 11 wherein the issuer verifies the validity of the authentication token by using the ARS.

20. The system of claim 11 wherein the ARS is configured to extract the data known only to the chip from the authentication token, regenerate the cryptogram, and compare the regenerated cryptogram with the authentication token.

21. The system of claim 11 further comprising mechanisms for submission of both authenticated transaction authorization requests and unauthenticated transaction authorization requests to the issuer.

22. A method for remote authentication of a customer who participates in an electronic transaction using a network access device, the method comprising:

providing the customer with an integrated circuit chip that has customer-identifying data;

providing a reader that is linkable to the customer's network access device and can communicate with the chip;

using an authentication request server (ARS), which is linked to the electronic network and can communicate data to the reader, to receive transaction specific information and to communicate transaction specific data to the reader;

using the reader to communicate the transaction specific data to the chip and to instruct the chip to generate a cryptogram based on at least a portion of the transaction specific data and at least a portion of the customer-identifying data;

using the reader to generate an authentication token based on at least part of the cryptogram generated by the chip;

using the ARS to validate authentication token;

generating an AAV upon validation of the authentication token and transporting the AAV over the electronic network in an Universal Cardholder Authentication Field (UCAF) message to the issuer.

23. The method of claim 22, wherein the transaction specific data communicated to the reader; comprises a challenge based on the transaction specific information.

24. The method of claim 22 wherein using the reader to generate an authentication token comprises generating an authentication token in a format that is compatible with 3-D Secure protocol message formats.

25. The method of claim 22 wherein the AAV is transported on the electronic network in an UCAF which has a 20 byte length.

26. The method of claim 22 wherein providing the customer with an integrated circuit chip and providing a reader comprise providing a chip and a reader that are co-disposed in a single physical package.

27. The method of claim 22 wherein the validation at the ARS comprises evaluating customer-identifying data in the authentication token by first rebuilding the data used by the chip to generate the cryptogram, next generating a replica cryptogram from the rebuilt data, and then matching the authentication token with the replica cryptogram.

28. The method of claim 27 further comprising accessing a cardholder database that is accessible by ARS to retrieve stored customer information.

29. The method of claim 27 further comprising communicating a validation result to a requesting party.

30. The method of claim 27 wherein the validation at the ARS further comprises matching an application transaction counter received from the chip against previous values of the application transaction counter received from the chip and accordingly authenticating the transaction.